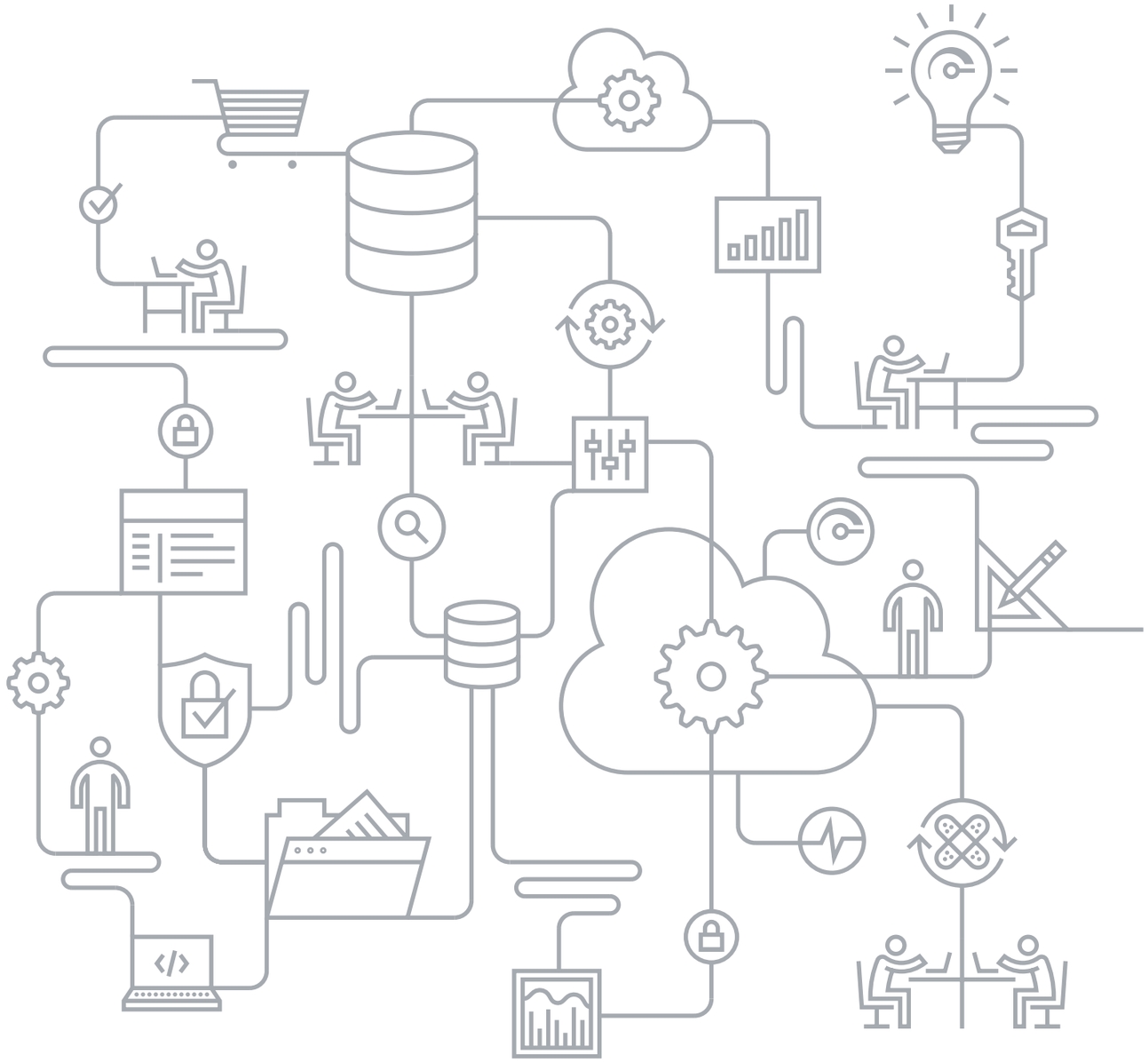
SIMPLIFYING VIRTUALIZATION WITH WINDOWS SERVER 2016 HYPER-V

Sterling Hammer



rackspace®

INTRODUCTION

Explore the Top Ten New Features and Enhancements

Microsoft® Hyper-V® Server offers the cost and efficiency advantages of virtualization, along with centralized management and control, built-in redundancy features like clustering and a unified set of orchestration tools.

And with its release of Windows® Server® 2016, Microsoft delivers even more Hyper-V features, including networking, storage and compute.

With so many features, it can be difficult to know where to begin. To help, we've put together our top-ten list. It offers guidance for getting these features installed and fully integrated into your environment so you can take full advantage of these efficiencies.

HYPER-V SPECIFIC FEATURES AND ENHANCEMENTS

1. Switch Embedded Teaming

Switch Embedded Teaming (SET) is a new method of utilizing teamed network interfaces with Hyper-V. Previously, with load balancing and failover teaming (LBFO), you were unable to take advantage of advanced features like remote direct memory access (RDMA). This increased the complexity of Hyper-V clusters and meant you needed dedicated network cards and ports for RDMA. Additionally, at the operating system level, this means you will no longer have a logical load balanced adapter underneath your virtual switch.

Additional benefits of SET are built-in support for Hyper-V network virtualization (NV-GRE and VxLAN), data center bridging (DCB), software defined networking quality of service (QoS), transmit-side checksum offloads (IPv4, IPv6, TCP), virtual machine queues (VMQ) and virtual receive-side scaling (RSS).

All NICs in a SET team must be the same make and model, and it does not support using different hardware vendors in the same team.

```
#
# Create a vmSwitch with SET
#
New-VMSwitch -Name SetSwitch -NetAdapterName "NIC SLOT 1","NIC SLOT 2" -EnableEmbed-
dedTeaming $true
#
# If you have RDMA enabled adapters
# Add host vNICs and make them RDMA capable
#
Add-VMNetworkAdapter -SwitchName SetSwitch -Name SMB_1 -managementOS
Add-VMNetworkAdapter -SwitchName SetSwitch -Name SMB_2 -managementOS
Enable-NetAdapterRDMA "vEthernet (SMB_1)","vEthernet (SMB_2)"
#
# Verify RDMA capabilities; ensure that the capabilities are non-zero
#
Get-NetAdapterRdma | fl *
#
# Most switches don't pass traffic class information on untagged VLAN traffic
# As a result make sure to assign a VLAN to your SMB vNICs
# You'll need to make sure you have this VLAN configured in your environment.
#
Set-VMNetworkAdapter -ManagementOS -VMNetworkAdapter SMB_1 -IsolationMode VLAN -De-
faultIsolationID 123
Set-VMNetworkAdapter -ManagementOS -VMNetworkAdapter SMB_2 -IsolationMode VLAN -De-
faultIsolationID 123
```

Learn more: https://technet.microsoft.com/en-us/library/mt403349.aspx#bkmk_sswitchembedded

2. Shielded Virtual Machines

Guarded fabric and shielded virtual machines (shielded VMs) bring a new level of security to Hyper-V virtualization in Windows Server 2016. Its primary focus is to protect tenant workloads from host compromises and malicious fabric administrators. A shielded VM is a generation 2 VM (supported on Windows Server 2012 and later) that contains a virtual TPM, is encrypted using BitLocker and, additionally, can only run on healthy and approved hosts within the fabric.

A guarded fabric contains one host guardian service (HGS), which is clustered for high availability, one or more guarded hosts and a set of shielded VMs. The HGS provides two services: attestation and key protection. The attestation service ensures that only trusted Hyper-V hypervisors can run shielded VMs while the key protection service provides the keys necessary to power them on and live migrate them between guarded hosts.

There are two specific attestation modes in the guarded fabric.

- **TPM-trusted attestation:** This offers the strongest possible protection but requires additional configuration steps and specific hardware with support for TPM 2.0 and UEFI 2.3.1 with secure boot.
- **Admin-trusted attestation:** This offers support for shielded VMs where host hardware that supports TPM 2.0 is not available. This is based on active directory security groups.

Shielded VMs provide a high level of security for your tenant workloads.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

Additionally, the Hyper-V VM you would like shielded must be at least configuration version 8.0.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server

3. PowerShell Direct

PowerShell® Direct allows you to run PowerShell commands on your Windows® 10 or Windows® Server 2016 VMs directly from the hypervisor host regardless of your network configuration or remote management settings. This can be accomplished by targeting the VM when using New-PSSession, Invoke-Command and Enter-PSSession.

```
#
# Enter an interactive session
#
Enter-PSSession -VMName <VMName>
Enter-PSSession -VMId <VMId>
#
# Exit the session
#
Exit-PSSession
#
# Run a single command
#
Invoke-Command -VMName <VMName> -ScriptBlock { cmdlet }
Invoke-Command -VMId <VMId> -ScriptBlock { cmdlet }
#
# Run a script
#
Invoke-Command -VMName <VMName> -FilePath C:\location\script_path\script.ps1
Invoke-Command -VMId <VMId> -FilePath C:\location\script_path\script.ps1
```


rackspace®

Learn more: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/powershell-direct

4. Host Resource Protection

Host resource protection prevents one or multiple VMs from using more than their share of host resources by looking for excessive levels of activity. This prevents a single VM from degrading the performance of the host or other VMs. When the system detects a VM with excessive activity, the VM is given fewer resources. This feature is disabled by default but it can be enabled with Windows PowerShell.

```
#
# Enable host resource protection
#
Set-VMProcessor -VMName <VMName> -EnableHostResourceProtection $true
```

The Set-VMProcessor cmdlet has a variety of other switches available as well.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows

5. Virtual Machine Load Balancing

Virtual machine load balancing is a new feature within failover clustering that enables VMs to balance across a cluster for maximum efficiency and resource utilization. It will identify over-committed nodes and will re-distribute tenant VMs to under-committed nodes. Previously, this feature was only available to those who utilized Virtual Machine Manager.

It utilizes Live Migration for zero-downtime migration to under-committed nodes. And it calculates this usage by identifying VM memory pressure and CPU utilization on the nodes. This feature is also enabled by default on all Hyper-V failover clusters. The thresholds can be adjusted based on your deployment configuration.

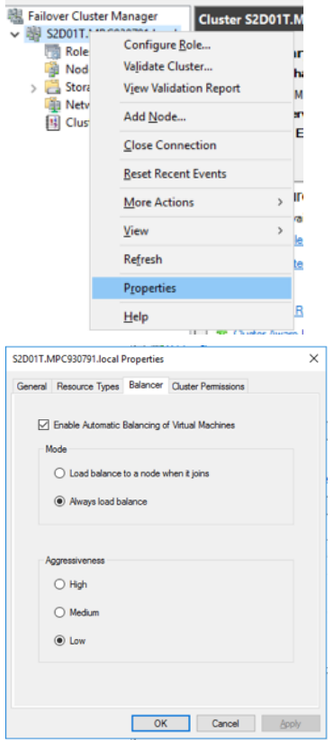
You can adjust the aggressiveness of balancing with the following PowerShell:

```
#
# The values are as follows:
# 1 (default)   Low Move when host is more than 80% loaded
# 2 Medium  Move when host is more than 70% loaded
# 3 High    Move when host is more than 60% loaded
#
(Get-Cluster).AutoBalancerLevel = <value>
```

Auto load balancing can also be disabled with the following:

```
#
# The values are as follows:
# 0 Disabled
# 1 Load balance on node join
# 2 (default)   Load balance on node join and every 30 minutes
#
(Get-Cluster).AutoBalancerMode = <value>
```

The following can also be completed in the Cluster Administrator:

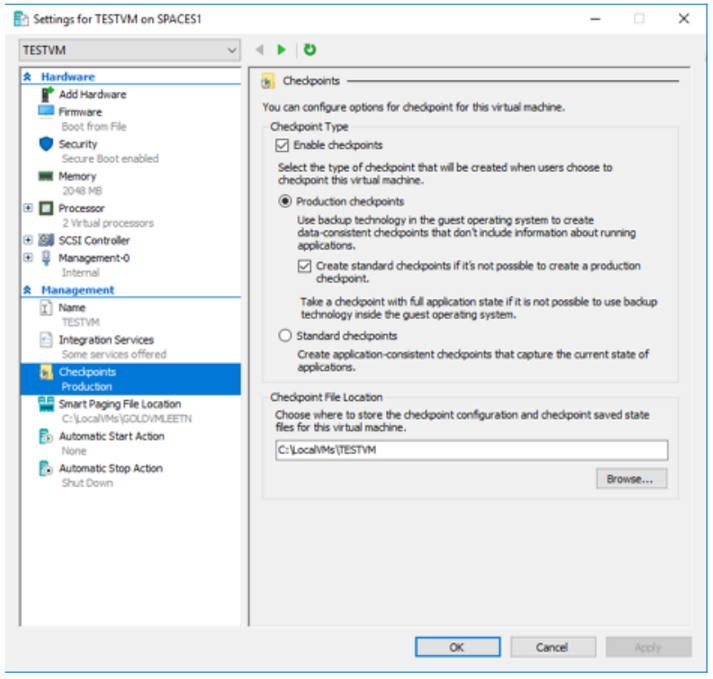


Learn more: https://technet.microsoft.com/en-us/windows-server-docs/failover-clustering/vm-load-balancing-overview

6. Production Checkpoints

Production checkpoints are essentially point-in-time images of a VM. Production checkpoints are based on backup technology inside the guest operating system instead of saved state. For Windows guests, VSS is utilized — while for a Linux file system, buffers are flushed to create a checkpoint that's consistent with the file system. This is a new feature but does not replace saved state checkpoints; however, they are enabled by default for new VMs. Standard checkpoints by contrast are intended more for development and test scenarios and are not as robust as production checkpoints.

These settings can be configured in Hyper-V manager under the VM settings.



Learn more: https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows

7. VM Configuration File Updates

Previously, on Windows Server 2012, the VM configuration files could become corrupt in certain situations. With Windows Server 2016, the file format has been improved to make reading and writing config files more efficient. The format makes data corruption less likely if a storage failure of some sort occurs. These are now in .vmcx format and editing them is not supported.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows

GENERAL WINDOWS IMPROVEMENTS

8. Simplified SMB Multichannel

SMB multichannel is not a new feature, but previously it required additional configuration in terms of hardware as well as network. For example, you would need additional hardwired NICs (preferably that supported RDMA) in addition to multiple network subnets. Windows Server 2016 simplifies this implementation so that the following occurs:

- Failover clustering will automatically detect NICs that are using the same subnet and/or switch
- You can utilize link local IPv6 addresses (fe80) for SMB Multichannel
- Multichannel is enabled automatically

The addition of SET means that you can now configure SMB multichannel "virtual" NICs on your high bandwidth connections that are RDMA enabled. SMB multichannel provides significant performance benefits with Hyper-V clusters.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/failover-clustering/smb-multichannel

9. Storage Spaces Direct

Storage Spaces Direct (S2D) creates a converged scenario with reduced complexity compared to previous versions. It utilizes industry-standard servers with local drives to create highly available and scalable software-defined storage at lower cost compared to SAN or NAS arrays.

With S2D, the fastest drives are utilized for cache (for example, NVMe and SSD drives). It's recommended to have 10% of your total spinning disk pool for caching.

S2D takes full advantage of RDMA NICs for increased throughput between host nodes. This, combined with the caching layer, offers a high level of performance for relatively low cost.

S2D offers QoS settings to ensure overly busy virtual machines do not consume a vast amount of storage I/O.

Learn more: https://technet.microsoft.com/windows-server-docs/storage/storage-spaces/storage-spaces-direct-overview

10. Failover Cluster Fault Domains

Both S2D and Storage Replica currently utilize Failover Cluster Fault Domains. This allows you to specify your fault domains from the chassis level all the way up to the site level. Fault domains are sets of hardware that share a single point of failure. To properly handle faults, you should have multiple fault domains at that level. For example, if you have a four-node cluster and two of the nodes are in rack A and two of the nodes are in rack B, you should define that within a fault domain.

This is managed within PowerShell and can be specified on the command line or with an XML file.

Learn more: https://technet.microsoft.com/en-us/windows-server-docs/failover-clustering/fault-domains

Trust Rackspace

Get a flexible IT infrastructure that can scale on demand while providing you with the performance, security and control you are used to. Rackspace Private Cloud combines Microsoft technologies of Hyper-V and Systems Center with our cloud expertise to deliver ongoing architecture, security and 24x7x365 operations backed by Microsoft-certified engineers and architects.

ABOUT RACKSPACE

Rackspace, the #1 managed cloud company, helps businesses tap the power of cloud computing without the complexity and cost of managing it on their own. Rackspace engineers deliver specialized expertise, easy-to-use tools, and Fanatical Support® for leading technologies developed by AWS, Google, Microsoft®, OpenStack®, VMware® and others. The company serves customers in 120 countries, including more than half of the FORTUNE® 100. Rackspace was named a leader in the 2017 Gartner® Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide and has been honored by Fortune®, Forbes® and others as one of the best companies to work for.

Learn more at www.rackspace.com or call us at **1-800-961-2888**.

PRI-CWP-Microsoft_Private_Cloud-_Ten_Hyper-V_Features_Whitepaper-5996-v02

JULY 14, 2017